



Sonnenschein

Overview of California Privacy Laws

**Reece Hirsch, Partner
Sonnenschein Nath & Rosenthal LLP**

**Protecting Privacy Online: A California Identity Theft
Summit
April 11, 2007**

California -- The Cutting Edge of Privacy Regulation

- California continues to be a trend-setter in privacy and identity theft law.
- *A de facto* national standard.
- CA has often been a first-adopter of new types of laws that are later passed by other states, such as:
 - Social Security number disclosure
 - Security breach notification

The ChoicePoint Incident

- Appears to be a watershed event in privacy regulation (and litigation).
- ChoicePoint, Inc. – one of the largest brokers of consumer data.
- By establishing at least 50 fake business accounts with ChoicePoint, criminals engaged in a massive identity theft scheme.
- ChoicePoint has identified at least 700 individuals who have been ID theft victims or attempted victims.

The ChoicePoint Incident

- February 16, 2005 – ChoicePoint announces that it has sent notices to 35,000 Californians.
 - Ultimately learns that financial records of more than 163,000 consumers sold to possible identity thieves.
 - Notification process driven by California S.B. 1386.

The Aftermath

- Sen. Dianne Feinstein introduces a security breach notification law in the Senate that parallels CA SB 1386 (S. 115).
- Attorneys General from 38 states send letters to ChoicePoint demanding notification of affected consumers.
- February 2006 – ChoicePoint agrees to pay \$10 million fine, the largest civil penalty in the FTC's history.
 - Also must create \$5 million fund for “consumer redress.”

State Legislative Reaction

- As of February 2006, the National Conference of State Legislatures reports on status of state security breach notification laws:
 - 2006: 25 bills introduced in 13 states.
 - 2005: 27 laws enacted in 22 states, 70 more bills introduced.
- Current total -- 35 states have enacted some form of breach notification law.
- Most are modeled after California's SB 1386.

The Lessons of ChoicePoint

- A sophisticated approach to privacy and security compliance is necessary, particularly for large companies that maintain databases of personal information, because:
 - Identity thieves are becoming very sophisticated.
 - The potential damages (class action litigation, stock price, reputation, etc.) are enormous.

Security Breach Notification Law

- Cal. Civil Code Section 1798.82.
- First-of-its-kind California security breach reporting law, requiring that:
 - any person or business conducting business in California
 - must report any breach of security
 - resulting in disclosure to an unauthorized person
 - of personal information in electronic form.

Personal Information

- Section 1798.82 applies only to personal information of California residents.
- Does not apply if data is encrypted.
- Defined as:
 - First name or first initial; and
 - Last name; and
 - Either Social Security number, driver's license number, or account number, credit or debit card number (with access code or password).

Security Breaches

- Good faith use of data by employees for business purposes generally is not a security breach.
- Company must notify affected individuals if it “reasonably believes” that personal information has been acquired by an unauthorized person.

Notification

- Company must disclose the breach to affected California residents “in the most expedient time possible and without unreasonable delay.”
- Content of notice is not specified, but may be in written or electronic form.

Recommended Practices

- California Office of Privacy Protection issued recommended practices document on October 10, 2003.
- <http://www.privacy.ca.gov/recommendations/secbreach.pdf>
- Notification recommended within 10 days of breach.
- Theft or loss of laptops triggers notice.
- Recommended encryption: NIST's Advanced Encryption Standard.

Contracting Issues

- **Obligation to report security breaches under vendor agreement**
 - **Has vendor agreed to security incident reporting?**
 - **Coordinating notification process under Cal. Civ. Code Section 1798.82**

Notification Challenges

- Managing telephone inquiries from notice recipients.
- Providing information regarding credit bureau credit checks and fraud alerts.
- Should you provide a credit monitoring service?
- Coordinating with law enforcement.

Class Action Lawsuits

- Any customer injured by a violation of Section 1798.82 may bring a civil action to recover damages.
- An invitation to class action lawsuits?

Proposed Amendments

- **A.B. 372 (Rep. Mary Salas, D) – Would allow state Attorney General to seek a civil penalty payable to the state of up to \$2,500 per violation.**
- **A.B. 512 (Rep. Sally Lieber, D) – Would add unencrypted “private medical and health care records” to definition of “personal information.”**

Proposed Amendments

- S.B. 364 (Sen. Joe Simitian, D) – Would lower the threshold for when government agencies may utilize substitute notice.
 - Current cost threshold of \$250,000 would be lowered to \$100,000.

The Ten Most Common Mistakes In Responding To A Security Breach

1. Failing to Understand Your Legal Obligations

- Understand whether you are legally obligated to notify
 - Don't overreact
 - Can't “unring the bell” once a notification letter has been sent.
- Remember that state breach notification laws differ.

Incident Response Legal Issues

- Is the company legally required to notify under applicable state breach notification laws?
 - Understand the triggers
 - Is “personal information” involved?
 - Has a “security breach” actually occurred?
 - Varying causation standards:
 - Is there a “reasonable belief” that information has been acquired by an unauthorized person (California)?
 - Is there a “likelihood of harm” (Delaware)?

Incident Response Legal Issues

- Legal obligation to notify is only the beginning of the analysis.
 - How would this incident be viewed by customers, public and press if it came to light?
 - When is notification an ethical/corporate citizenship (as opposed to legal) obligation?

2. Failing To Follow Your Incident Response Plan

- In the heat of a crisis, organizations often forget that they adopted a security incident response plan.
- If regulators or plaintiffs in a class action charge that you acted unreasonably, being able to demonstrate that you followed a reasonable security incident response plan is a good way to show otherwise.

3. Failure to Follow Forensic Procedures

- **The ideal outcome – catching the bad guy and recovering the data before customers are harmed.**
- **Failure to follow proper computer forensic procedures may erase or spoil evidence.**
- **Identify internal or external forensic resources in advance.**

4. Failing to Coordinate With Law Enforcement

- Consider whether it's appropriate to notify law enforcement.
 - Choose the right agency:
 - Local high tech crimes task force
 - FBI
 - Secret Service
 - National Infrastructure Protection Service
 - Don't use half-hearted law enforcement investigation as an excuse to delay notification!

5. Coordinate With Credit Reporting Agencies

- Consider notifying credit reporting agencies before sending a notice to customers.
- If a police report has been filed, customers may find it useful to receive a copy.
- Consider free credit monitoring for a specified period (one year), particularly if there has been actual fraud or identity theft.

Other Common Incident Response Mistakes

6. Drafting a notification letter in a manner that inappropriately concedes wrongdoing.

Common Incident Response Mistakes

7. Failure to train workforce to spot and report a security breach immediately.
8. Failure to involve legal counsel at the earliest stages.

Common Incident Response Mistakes

9. Failure to require prompt security breach notification in agreements with vendors/agents.
10. Organize your incident response team in advance so that you're prepared to respond quickly.

Social Security Number Law

- Cal. Civil Code Section 1798.85
- Limits use and disclosure of SSNs
- Affects any individual or nongovernmental entity doing business in California
- Intended to limit identity theft and restrain consumer reporting agencies that are accessing personal information through SSNs

SSN Disclosure Law

- **Five prohibited uses of SSNs:**
 - **May not publicly post or display an SSN**
 - **May not print an SSN on any card required for access to products or services (insurance cards, employee badges)**
 - **May not require an individual to transmit SSN over Internet unless connection is secure or SSN is encrypted**

SSN Disclosure Law

- May not require an individual to use SSN to access website, unless an additional password or other authentication device must also be used to access site.

SSN Disclosure Law

- May not print an individual's SSN on any materials that are mailed to the individual, unless state or federal law requires SSN to be on document.
 - Exception: applications and forms sent by mail, including documents:
 - sent as part of an application or enrollment process
 - To establish, terminate or amend account
 - To confirm accuracy of SSN

SSN Disclosure Law

- Statute does not prevent:
 - Collection, use or release of an SSN if required by state or federal law
 - Use of an SSN for internal verification or administrative purposes

Online Privacy Notice Law

- Assembly Bill 68, the Online Privacy Protection Act of 2003
- Effective July 1, 2004
- Requires an operator of a commercial website or online service that gathers “personally identifiable information” (PII) to provide notice of privacy policy so that consumers are informed of potential disclosure, sale or sharing of information

Online Privacy Notice Law

- “Personally identifiable information” is individually identifiable information collected:
 - Online
 - By an operator of a commercial website or online service
 - Maintained in accessible form

Online Privacy Notice Law

- “Personally identifiable information” includes:
 - First and last name
 - Home or other address, including street name and name of city
 - E-mail address
 - Telephone number
 - Social Security number
 - Any identifier permitting physical or online contact
 - Any information concerning a user maintained in combination with one of these identifiers

Online Privacy Notice Law

- Privacy policy must be conspicuously posted and:
 - Identify categories of PII collected and third parties with whom PII may be shared
 - Describe process for notifying consumers of material changes to policy

Online Privacy Notice Law

- If operator maintains a process for individual to review and request changes to PII, describe that process
- Identify the effective date of the policy

Online Privacy Notice Law

- “Conspicuously posted” means:
 - Text of policy on homepage or first significant page after entering website
 - Icon link to policy on homepage or first significant page
 - Must include the word “privacy”
 - Color must contrast with background or be otherwise distinguishable

Online Privacy Notice Law

- Text link on homepage or first significant page:
 - Must include the word “privacy”
 - Must be in capital letters equal to or larger than surrounding text
 - Larger type than surrounding text or in contrasting type, font or color

Online Privacy Notice Law

- Any other functional hyperlink that is so displayed that a reasonable person would notice it.
- Any other reasonably accessible means of making policy available to user of an online service.

Reasonable Security Practices

- In the world of privacy regulation, isolated incidents can have far-reaching effects.
- A.B. 1950 was prompted by an incident in which a TV network used a file cabinet containing personal information of network employees as a prop during filming of a program.

Reasonable Security Practices

- Signed into law by Governor Schwarzenegger on Sept. 29, 2004. Effective January 1, 2005.
- Added Civil Code Section 1798.81.5.
- Basic mandate is fairly simple:
 - A business that owns or licenses personal information about a California resident shall
 - Implement and maintain reasonable security procedures and practices

Reasonable Security Practices

- Appropriate to the nature of the information
- To protect the personal information from unauthorized access, destruction, use, modification or disclosure.

Personal Information

- “Personal information” means:
 - an individual’s first name or first initial
 - AND last name
 - IN COMBINATION WITH one of the following, when either the name or the other data elements are not encrypted or redacted:
 - Social Security number
 - Driver’s license number or CA Identification Card number

Personal Information

- Account number, credit card number , in combination with any required security code, access code or passcode that would permit access to a financial account.
- Medical information.
- Does not include information that is publicly available through federal, state or local government records.

Owns or Licenses Personal Information

- Includes personal information that a business retains as part of internal customer account or for purposes of transactions with its customers.
- Does this include HR data regarding a company's employees?
 - Not clear from statute
 - Should probably assume its included absent further guidance

Contracting Requirement

- A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party
- Must require by contract that the party implement and maintain reasonable security procedures and practices
 - Appropriate to nature of the information
 - To protect the information from unauthorized use or disclosure

Contracting Requirement

- Only applies when disclosures are pursuant to a contract.
- Many common disclosures of personal information may be permitted by law and are engaged in without a contract.
- AB 1950 would not require that parties enter into a contract when they didn't previously.
- No sample contract language has been issued.

Not Subject to A.B. 1950

- A provider of health care, health care service plan or contractor regulated by the Confidentiality of Medical Information Act.
- A financial institution regulated under the Financial Code or S.B. 1.
- A HIPAA covered entity
- An entity subject to confidentiality provisions of Vehicle Code regarding driver's license info.

Not Subject to A.B. 1950

- A business that is regulated by a state or federal law providing greater protection for personal information.
- AB 1950 is a gap-filler – intended to cover businesses that are not regulated under industry-specific CA privacy laws.

Relationship to S.B. 1386

- AB 1950 complements SB 1386, CA's security breach notification law.
- Both use same definition of personal information (except that AB 1950 adds "medical information").
- SB 1386 created an incentive for businesses to adopt reasonable security practices – AB 1950 imposes an affirmative legal obligation to do so.

The Big Question

- What are reasonable security procedures and practices?
- No specific guidance on security practices – lets businesses exercise their own judgment as to what level of security is appropriate.

Industry-Specific Privacy Laws

- Confidentiality of Medical Information Act (Civil C. § 56 *et seq.*)
- Insurance Information and Privacy Protection Act (Ins. C. § 791 *et seq.*)
- Financial Information Privacy Act (Fin. C. § 4050 *et seq.*)

Other Privacy Laws

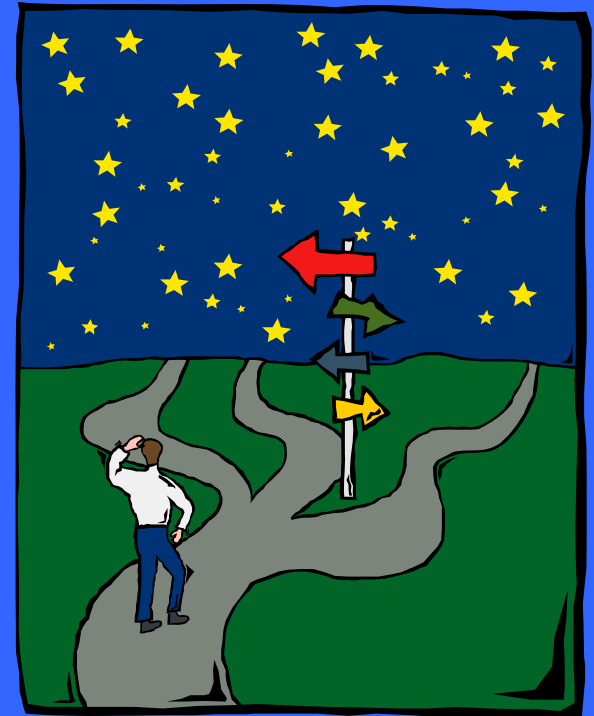
- Marketing Disclosure (“Shine the Light”) Law (Civil C. §1798.83-.84)
- Telephone Record “Pretexting” (Penal C. §638)

California Constitution

- *All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.*
-Article 1, Section 1 of the California Constitution

What's Next?

- For a glimpse into the future of state and federal privacy and identity theft legislation, keep an eye on the California Legislature.
- Possible new subjects of regulation:
 - RFID
 - Outsourcing





Sonnenschein

For further information contact:

Reece Hirsch

Sonnenschein Nath & Rosenthal LLP

415.882.5040

rhirsch@sonnenschein.com